Passage at Content Distribution And End-to-End DRM

for DSTAC

March 14, 2015

Brant Candelore
Passage Architect / Security Specialist / Sr. Staff Member
UX Technology Center – San Diego
Sony Electronics Inc.

What is Passage

See Classic “Passage Technical Overview” PowerPoint presentation

Passage is an enabler - for new distribution paradigms - all while preserving the operators’ capital investment in legacy set-top boxes and distribution equipment!

Why Passage

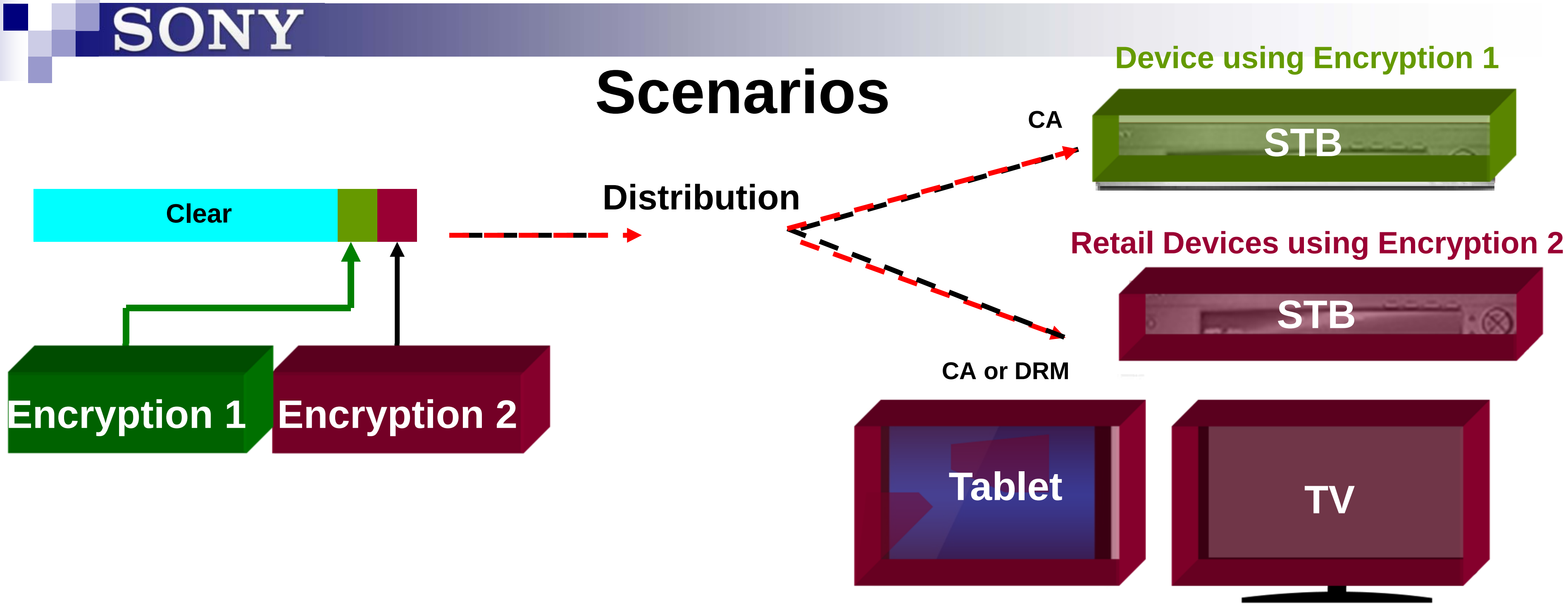
a) Alternate scrambling of the critical packets, e.g. AES-128 vs. DES or CSA

b) Legacy CA can co-exist new CA or DRM

- Alternate security (software vs. hardware-based CAS)
- Alternative key management (content rights vs. entitlements)
- Alternative Root of Trust (Crypto vs. Key Ladder vs. Software)
- Alternative to key sharing (Simultcrypt) which may not be possible or desirable

Result: Linear content can be encrypted with DRM same as Web services which might help the transition to “all-IP” services

Scenarios



Scenario	Encryption 1	Encryption 2	Comment
1	Legacy CA	Alternate CA	“Classic” Passage
2	Legacy CA	DRM	End-to-End DRM
3	DRM	DRM	Multicast IP with independent keys

Enabling Sony Passage at the Point of Content Distribution

- Potential to facilitate Passage throughout content distribution ecosystem

Content Distribution

Content is currently delivered in the following ways to headends:

a) Back-haul Delivery Networks, e.g. Comcast Wholesale: HITS and Fiber
   - Networks get content from Programmers

b) Direct from Programmers

c) Local content

Methods a) and b) can benefit from doing Passage at the point of distribution. Existing headend equipment can be utilized. If Programmers, Method b) enabled Passage, then a) might accommodated. See following "Commercial Distribution" slides

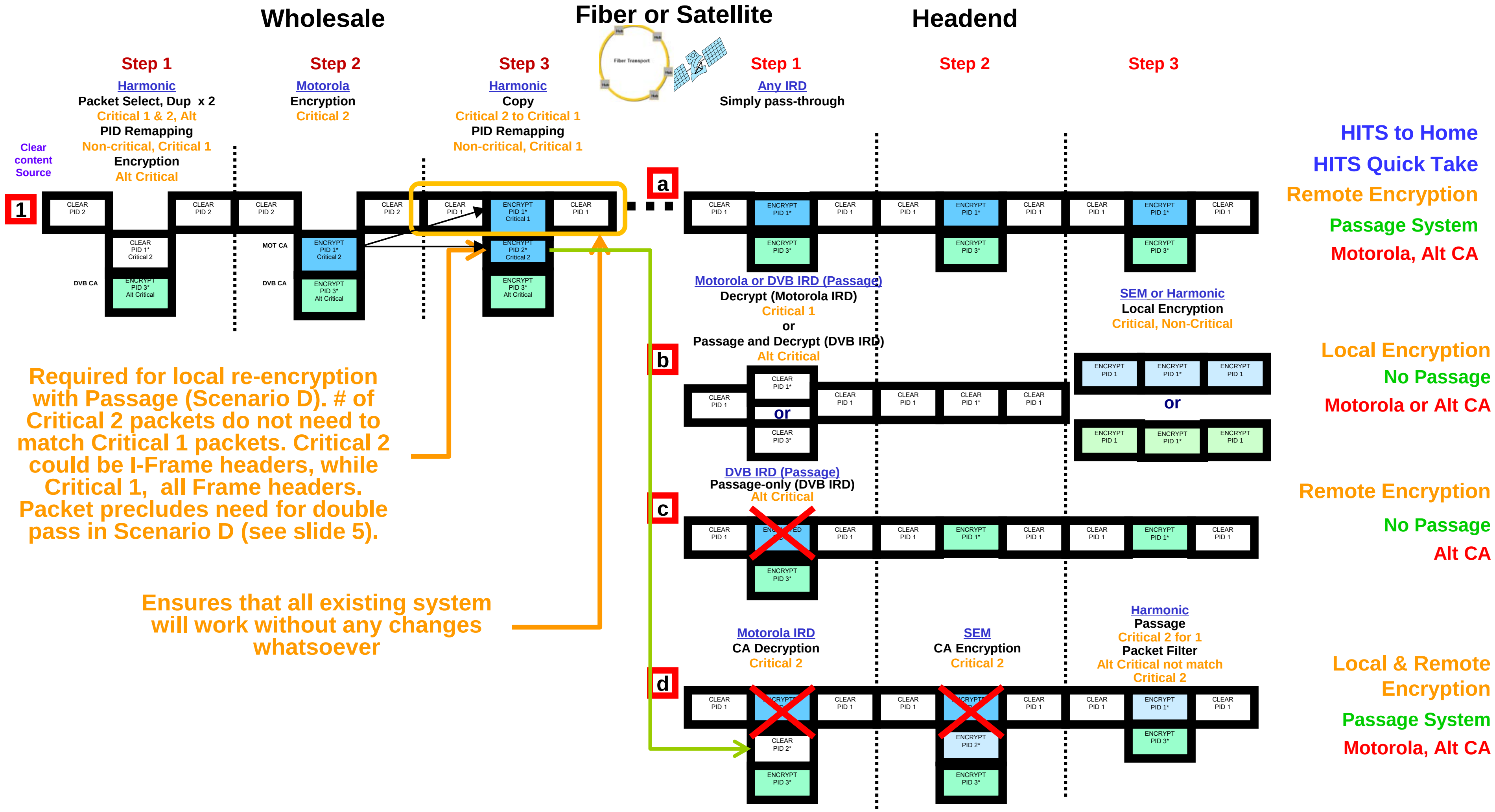
c) must be Passage-encoded locally

There are a number of different types of headend systems which must be considered.

a) Digital Turnaround	
b) Local Encryption	(no Passage)
c) Remote Encryption	(no Passage)
d) Local and Remote Encryption	

All can be accommodated!

Commercial Distribution Scenario using Passage (3 Critical Packets)



Wholesale

Fiber or Satellite

Headend

Step 1
Harmonic
Packet Select, Dup x 2
Critical 1 & 2, Alt
PID Remapping
Non-critical, Critical 1
Encryption
Alt Critical

Step 2
Motorola
Encryption
Critical 2

Step 3
Harmonic
Copy
Critical 2 to Critical 1
PID Remapping
Non-critical, Critical 1

Step 1
Any IRD
Simply pass-through

Step 2

Step 3

Clear content Source

Motorola or DVB IRD (Passage)
Decrypt (Motorola IRD)
Critical 1
or
Passage and Decrypt (DVB IRD)
Alt Critical

SEM or Harmonic
Local Encryption
Critical, Non-Critical

DVB IRD (Passage)
Passage-only (DVB IRD)
Alt Critical

Motorola IRD
CA Decryption
Critical 2

SEM
CA Encryption
Critical 2

Harmonic
Passage
Critical 2 for 1
Packet Filter
Alt Critical not match
Critical 2

Required for local re-encryption with Passage (Scenario D). # of Critical 2 packets do not need to match Critical 1 packets. Critical 2 could be I-Frame headers, while Critical 1, all Frame headers. Packet precludes need for double pass in Scenario D (see slide 5).

Ensures that all existing system will work without any changes whatsoever

a: HITS to Home
HITS Quick Take
Remote Encryption
Passage System
Motorola, Alt CA

b: Local Encryption
No Passage
Motorola or Alt CA

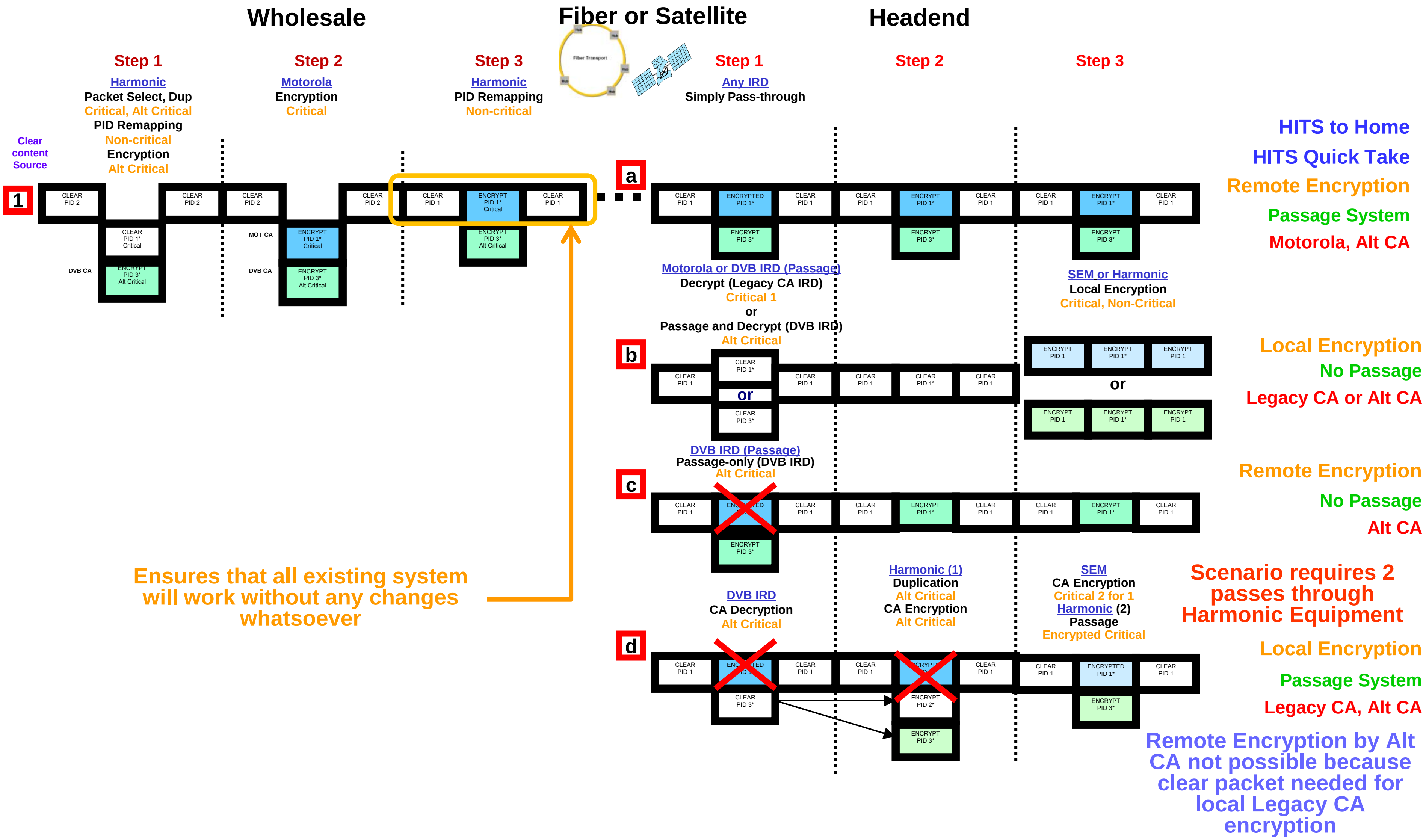
c: Remote Encryption
No Passage
Alt CA

d: Local & Remote Encryption
Passage System
Motorola, Alt CA

Legend:

*Critical Packet

Commercial Distribution Scenario using Passage (2 Critical Packets)



Wholesale

Fiber or Satellite

Headend

Clear content Source

Step 1
Harmonic
Packet Select, Dup
Critical, Alt Critical
PID Remapping
Non-critical
Encryption
Alt Critical

Step 2
Motorola
Encryption
Critical

Step 3
Harmonic
PID Remapping
Non-critical

Step 1
Any IRD
Simply Pass-through

Step 2

Step 3

Motorola or DVB IRD (Passage)
Decrypt (Legacy CA IRD)
Critical 1
or
Passage and Decrypt (DVB IRD)
Alt Critical

SEM or Harmonic
Local Encryption
Critical, Non-Critical

DVB IRD (Passage)
Passage-only (DVB IRD)
Alt Critical

DVB IRD
CA Decryption
Alt Critical

Harmonic (1)
Duplication
Alt Critical
CA Encryption
Alt Critical

SEM
CA Encryption
Critical 2 for 1
Harmonic (2)
Passage
Encrypted Critical

Ensures that all existing system will work without any changes whatsoever

HITS to Home
HITS Quick Take
Remote Encryption
Passage System
Motorola, Alt CA

Local Encryption
No Passage
Legacy CA or Alt CA

Remote Encryption
No Passage
Alt CA

Scenario requires 2 passes through Harmonic Equipment

Local Encryption
Passage System
Legacy CA, Alt CA

Remote Encryption by Alt CA not possible because clear packet needed for local Legacy CA encryption

Legend:

*Critical Packet

End-to-End DRM

- Treating linear content like IP-delivered DRM content

End-to-End DRM

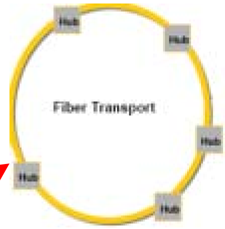
- Capitalize on high quality linear content sent to legacy receivers
  - Customer buys inexpensive QAM tuner cards or QAM tuner USB stick
- Eliminate the need for CAS-to-DRM bridging. Bridging has the following issues:
  - OCUR/BOCUR solutions using CAS, e.g. CableCARD, are expensive
  - Rights and access criteria may be lost in “translation” using DTCP/IP and DLNA
  - Possible clear content or key trans-encryption exposure vulnerability
- DRM content (sent from linear programming) can be managed in the same way as that delivered strictly over IP
- Provides greater control over broadcast content
- Enables new business opportunities and models
- DRM packet could originate at Programmer Passage-enable facility. This minimizes the multiplexer changes at Distribution Networks and Headends

End-to-End DRM – To PC

Headend Scenarios

Selective Multiple Encryption

CLEAR not-encrypted PID 100	LEGACY Critical CA encrypted PID 100	WMDRM Critical encrypted PID 101	Widevine Critical encrypted PID 102



Storage & Distribution Scenarios

CLEAR not-encrypted PID 100	Widevine Critical encrypted PID 100

IP Distribution in the home, e.g.
MOCA or Wi-Fi

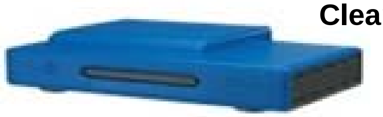
AverMedia PCI CARD

Clear QAM tuner to USB

Hauppauge 950Q USB2 QAM Tuner
Clear QAM tuner to USB

Clear QAM Tuners can be used since
DRM decryption is done in Client

SiliconDust Homerun Tuner
Clear QAM tuner to IP

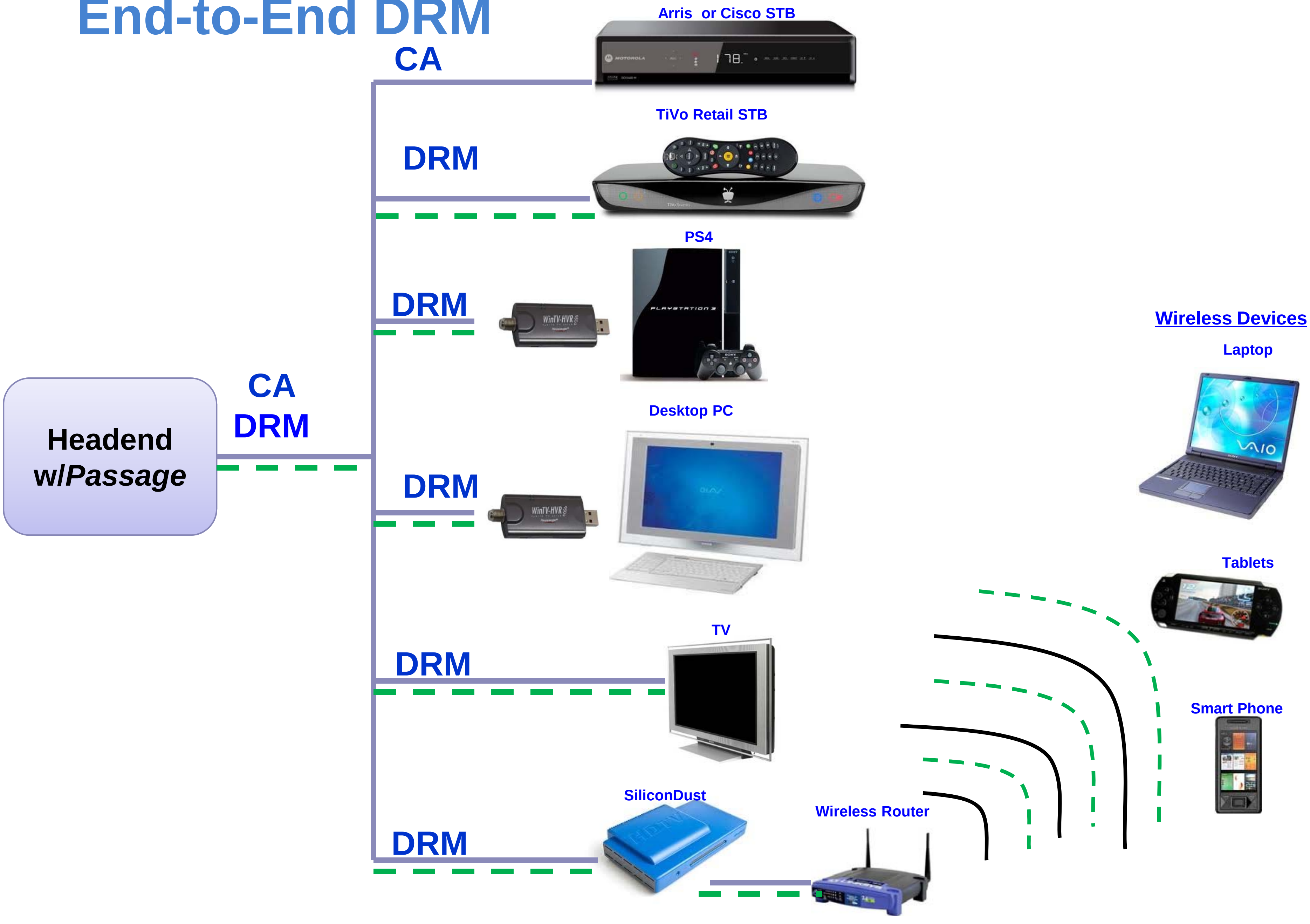


PC browsing
of MSO
content

Direct reception by PC using existing PCI tuner board
(decoding done by multi-core PC)

- No need for CA decryption and re-encryption
- Passage can be managed by client on PC, TV, or Tablet

End-to-End DRM



Headend w/*Passage*

CA

DRM

CA

Arris or Cisco STB

DRM

TiVo Retail STB

DRM

PS4

DRM

Desktop PC

DRM

TV

DRM

SiliconDust

Wireless Router

Wireless Devices

Laptop

Tablets

Smart Phone